

CLAIMS

We claim:

1. A method for permitting access to applications, said method comprising:
registering a first restricted application with at least one additional restricted application;
5 and

in response to a user performing only a single sign-on for said first restricted
application,

providing access to said first restricted application for said user;

presenting to said user information identifying said at least one additional restricted
10 application; and

in response to said user's selection, providing access to said at least one additional
restricted application.

2. The method of Claim 1, wherein said registering further comprises:

15 performing a single registration for all authorized users of said first restricted
application.

3. The method of Claim 1, wherein said registering further comprises:

performing a plurality of registrations,

20 for a plurality of groups of authorized users of said first restricted application; and
providing an access level for each of said groups.

4. The method of Claim 1 wherein:

25 said first restricted application is an application other than merely a security
mechanism.

5. The method of Claim 1 wherein:

no additional key repository is required by said restricted applications.

6. The method of Claim 1 wherein:

said presenting further comprises said first restricted application sending a document in hypertext markup language.

5 7. The method of Claim 1, wherein said user's selection further comprises:

receiving via said first restricted application a selection signal from said user; and
in response to said selection signal, sending via said first restricted application a request for access to said at least one additional restricted application.

10 8. The method of Claim 7, wherein:

said user clicks a mouse button when a cursor is positioned over a predefined area of said presented information, to produce said selection signal.

9. The method of Claim 1, further comprising:

15 collecting stored information regarding a user and an appropriate level of access; and
sending to said user:

a token and

a redirect URL pointing to said at least one additional restricted application.

20 10. The method of Claim 9, wherein:

said token is encrypted; and

said token represents said appropriate level of access.

11. The method of Claim 1, wherein:

25 one of said restricted applications is an intranet web server.

12. The method of Claim 1, wherein:

one of said restricted applications is a portal.

13. The method of Claim 1, wherein:

one of said restricted applications is a web application.

14. A method for permitting access to applications, said method comprising:

5 registering a first restricted application with a second restricted application; and
in response to a user:

signing on to said first restricted application only,

and requesting access to said second restricted application,

automatically logging in to said second restricted application, for said user;

10 wherein:

no new key repository is required by said first and second restricted applications.

15. The method of Claim 14, wherein said automatically logging in further comprises:

under control of said second restricted application,

15 receiving from said first restricted application, a request to initiate said automatically
logging in;

sending to said user's client, via said first restricted application a response, having a
complete-automatic-log-in URL, and token;

receiving directly from said user's client a request, having said token; and

20 sending directly to said user's client a response, having authenticated session
information, and a welcome URL.

16. The method of Claim 15, further comprising:

in response to said request to initiate,

25 creating said token;

storing a copy of said token; and

associating said token with said request to initiate.

17. The method of Claim 15, further comprising:

verifying said token received from said user's client; and
establishing a relationship and access level for said user's client.

18. The method of Claim 15 wherein:

5 said token represents an appropriate level of access.

19. The method of Claim 14, further comprising:

under control of said first restricted application,

10 receiving from said user's client a request for access to said second restricted
application;

in response to said request for access, determining for said user, and said second
restricted application, what level of access should be granted; and

15 sending to said second restricted application a request to initiate said automatically
logging in.

20. A system for permitting access to applications, said system comprising:

means for registering a first restricted application with a second restricted application;
and

20 means for automatically logging in to said second restricted application, for a user;
wherein:

no additional key repository is required by said first and second restricted applications;
and

said means for automatically logging in is responsive to said user:

25 signing on to said first restricted application only,

and requesting access to said second restricted application.

21. The system of Claim 20, wherein said means for automatically logging in further
comprises:

means for receiving from said first restricted application, a request to initiate said

means for automatically logging in;

means for sending to said user's client, via said first restricted application, a response, having a complete-automatic-log-in URL, and a token;

means for receiving directly from said user's client a request, having said token; and

5 means for sending directly to said user's client a response, having authenticated session information, and a "welcome" URL or initial URL.

22. The system of Claim 21, further comprising:

10 means for creating said token;

means for storing a copy of said token; and

means for associating said token with said request to initiate.

23. The system of Claim 21, further comprising:

15 means for verifying said token received from said user's client; and

means for establishing a relationship and access level for said user's client.

24. The system of Claim 21, wherein:

said token could represent an appropriate level of access.

20

25. The system of Claim 20, further comprising:

means for receiving from said user's client a request for access to said second restricted application;

25 means for determining for said user, and said second restricted application, what level of access should be granted; and

means for sending to said second restricted application a request to initiate said means for automatically logging in.

26. A computer-usable medium, having computer-executable instructions for permitting

access to applications, said computer-usable medium comprising:

means for registering a first restricted application with a second restricted application;

and

means for automatically logging in to said second restricted application, for a user;

5 wherein:

no additional key repository is required by said first and second restricted applications;

and

said means for automatically logging in is responsive to said user:

signing on to said first restricted application only,

10 and requesting access to said second restricted application.

27. The computer-usable medium of Claim 26, wherein said means for automatically logging in further comprises:

means for receiving from said first restricted application, a request to initiate said

15 means for automatically logging in;

means for sending to said user's client, via said first restricted application, a response, having a complete-automatic-log-in URL, and token;

means for receiving directly from said user's client a request, having said token; and

20 means for sending directly to said user's client a response, having authenticated session information, and a welcome URL.

28. The computer-usable medium of Claim 27, further comprising:

means for creating said token;

means for storing a copy of said token; and

25 means for associating said token with said request to initiate.

29. The computer-usable medium of Claim 27, further comprising:

means for verifying said token received from said user's client; and

means for establishing a relationship and access level for said user's client.

30. The computer-usable medium of Claim 27, wherein:
said token represents an appropriate level of access.

31. The computer-usable medium of Claim 26, further comprising:

5 means for receiving from said user's client a request for access to said second
restricted application;
means for determining for said user, and said second restricted application, what level
of access should be granted; and
10 means for sending to said second restricted application a request to initiate said means
for automatically logging in.